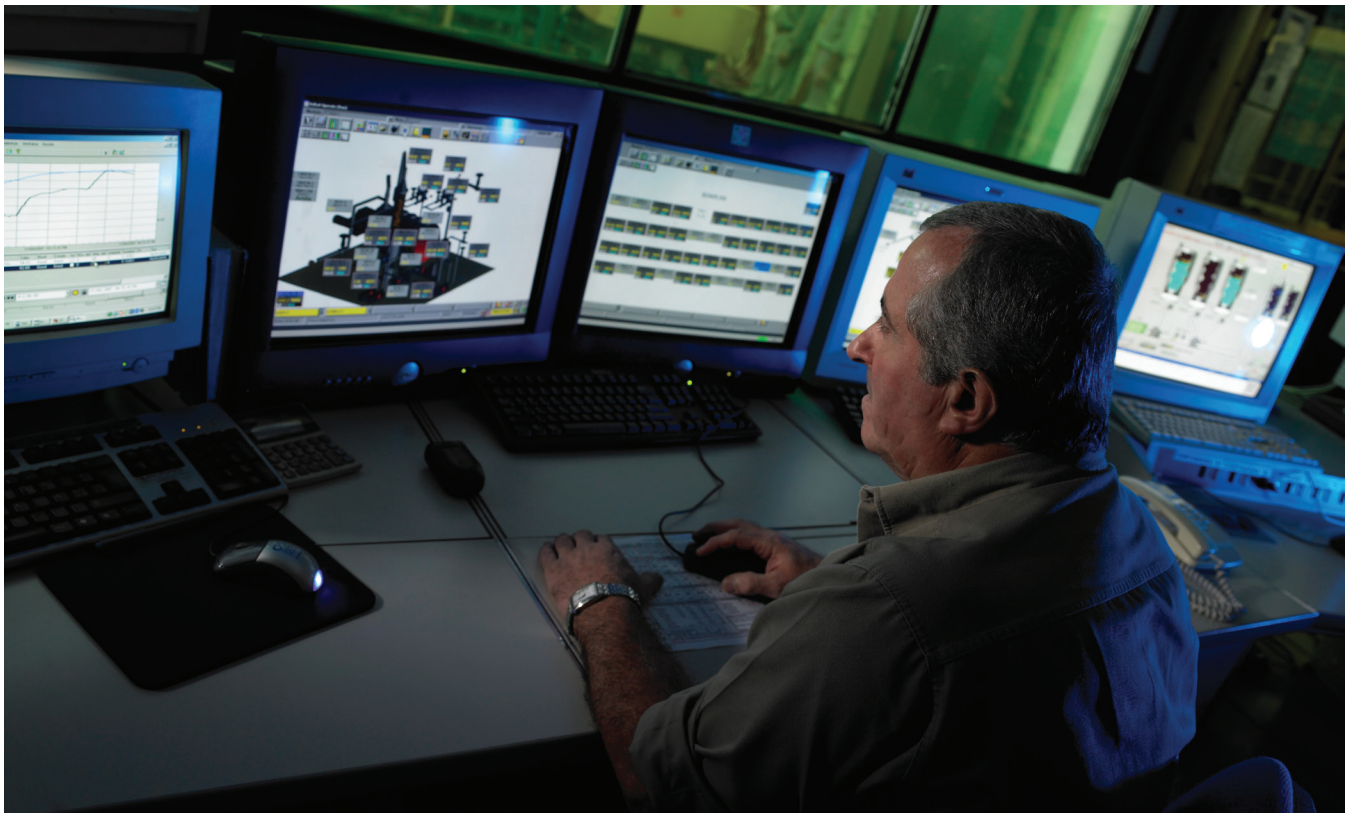
DeltaV™ Security Manual

Implementing Security on the DeltaV Distributed Control System



To protect this information this public version only provides the Table of Content information.

A full copy of this document will be provided upon request to your local DeltaV sales/support office.

For internal Emerson personnel: This document is available on the Global Sales Portal in the DeltaV Confidential Papers section.

© 2015 Fisher-Rosemount Systems, Inc. All rights reserved.

This manual is Emerson confidential and intended for use only by customers, employees, LBPs, and others who are responsible for providing security services to Emerson Process Management systems and products. It may be provided to potential customers as required to evaluate DeltaV security implementation. It does not require an NDA for distribution.

This manual must not be posted on public websites or redistributed, except as noted above, without permission from Emerson Process Management.

EMERSON™
Process Management

Table of Contents

1 Introduction 5
1.1 Purpose 5
1.2 Organization 5
1.3 Relevant documentation 5
1.3.1 Background reading 5
1.3.2 DeltaV documentation 6
1.3.3 Microsoft documentation 6
1.3.4 3rd party product documentation 6
1.4 Security and DeltaV system projects 7
1.5 Security Collaboration between IT and Operations Departments 8
1.6 Submitting Material for This Manual 10
1.7 Glossary 10
2 Security basics 12
2.1 Threats to control systems 12
2.2 Assets and compromises 12
2.3 Vulnerabilities 13
2.4 Performing a risk assessment 13
2.4.1 Summary security checklist 14
2.4.2 Defense-in-depth 15
2.4.3 Security Hardening 15
2.5 Protecting assets from threats 15
2.5.1 Overview 15
2.5.2 Principal safeguards 16
2.5.2.1 Security policies and procedures 16
2.5.2.2 Physical security 18
2.5.2.3 Cyber security perimeters 18
2.5.2.4 Encryption and digital signatures 19
2.5.2.5 Role-based access controls 20
2.6 Implementing DeltaV security 20
3 DeltaV security 21
3.1 Overview 21
3.2 DeltaV architecture 22
3.2.1 External access to DeltaV systems 22
3.2.1.1 DeltaV 2.5 network 22

3.2.1.1.1 Description 22
3.2.1.1.2 DeltaV 2.5 network connectivity 25
3.2.1.1.3 Using wireless in the DeltaV 2.5 network 26
3.2.1.1.3.1 Wireless Ethernet device security 28
3.2.1.1.4 The DeltaV 2.5 network perimeter security device 28
3.2.1.2 The DeltaV remote (RAS) network 29
3.2.1.3 The Process DMZ 30
3.2.1.4 Remote access applications 32
3.2.1.4.1 Overview 32
3.2.1.4.2 Microsoft Remote Desktop 33
3.2.1.4.3 DeltaV remotely accessible applications 34
3.2.1.4.4 DeltaV Firewall Configuration Information 35
3.2.2 DeltaV control system networks 39
3.2.2.1 DeltaV area control network (ACN) 39
3.2.2.1.1 Description 39
3.2.2.1.2 Emerson Process Management Smart Switches 40
3.2.2.1.2.1 Capabilities and operation 40
3.2.2.1.2.2 Management 41
3.2.2.1.3 DeltaV Controller Firewall 41
3.2.2.1.3.1 Capabilities and operation 41
3.2.2.1.3.2 Management 42
3.2.2.1.4 Connecting non-DeltaV computers to the ACN 42
3.2.2.1.5 Extending the ACN using wireless Ethernet bridges 43
3.2.2.2 SIS networks 43
3.2.2.2.1 Description 43
3.2.2.2.2 DeltaV SIS Intrusion Protection Device (SIS IPD) 44
3.2.2.2.2.1 Capabilities and operation 44
3.2.2.2.2.2 Management 45
3.2.2.2.3 SIS Engineering Workstations 45
3.2.2.3 *Wireless*HART segments 45
3.2.2.3.1 Description 45
3.2.2.3.2 Separation of maintenance workstations and wireless devices 47
3.2.2.3.3 WirelessHART device security 47
3.2.3 DeltaV Zones 47
3.2.4 DeltaV workstations 47
3.2.4.1 Physical security 47

3.2.4.2 Workstation security templates 48
3.2.4.3 Workstation locking 48
3.2.4.4 File system 48
3.2.4.5 Removable devices 49
3.2.4.6 Anti-Virus software 49
3.2.4.7 Workstation applications and services 50
3.2.4.7.1 Disabled services 50
3.2.4.7.2 Email 52
3.2.4.7.3 Internet Explorer 52
3.2.4.8 Workstation Data, Alarms, and Events 53
3.2.4.8.1 Data access 53
3.2.4.8.1.1 Control parameters 53
3.2.4.8.1.2 Data historians 54
3.2.4.9 Portable device security 54
3.2.5 Controller security 55
3.2.5.1 Physical security 55
3.2.5.2 Connection to the ACN 56
3.2.5.3 DeltaV Controller I/O protection 56
3.3 DeltaV functional security 56
3.3.1 User security 56
3.3.1.1 Account management 56
3.3.1.1.1 Centralized management of accounts 57
3.3.1.1.2 Account creation and maintenance 57
3.3.1.1.3 Account expiration 58
3.3.1.1.4 Removal of temporary accounts 59
3.3.1.1.5 Removal of unused accounts 59
3.3.1.2 Passwords 59
3.3.1.2.1 Composition 60
3.3.1.2.2 Default passwords 60
3.3.1.2.3 Expiration period 61
3.3.1.2.4 Expiration prompt 61
3.3.1.2.5 Reuse 61
3.3.1.3 Shared accounts 61
3.3.1.4 Installation-generated user accounts 62
3.3.1.5 Account activity logging 62
3.3.1.6 Logging into the DeltaV system 62

3.3.2 Security event handling 63
3.3.2.1 Event logging and reporting 63
3.3.2.1.1 General security event handling 63
3.3.2.1.2 User activities 63
3.3.2.1.3 Log of failed login attempts 63
3.3.2.2 Event monitoring 64
3.4 Security certifications 64
3.4.1 Vendor products 64
4 Patching 65
4.1 General patching policy 65
4.1.1 Operational impacts 66
4.1.2 Patch list management 68
4.1.3 Patching timeliness 69
4.1.4 Policies and procedures 70
4.2 Microsoft Windows updates 71
4.2.1 Introduction 71
4.2.2 Windows non-security updates 71
4.2.3 Security updates 71
4.3 DeltaV workstation hotfixes 72
4.4 DeltaV Controller and I/O hotfixes 73
5 Backups and disaster recovery 74
5.1 Overvie 74
5.2 Backup/Recovery capability 74
5.3 Backup strategy 75
6 Cyber security services 76
6.1 Standards, policies and procedures 76
6.2 Confidentiality agreements 76
6.3 Standards committees 76
6.4 Security contact 76
6.5 System change procedures 77
6.6 Incident Response Policies and Procedures 78
6.7 System hardening 78
6.8 Conducting security risk assessments 78
6.9 Use of troubleshooting tools 78

1 Introduction

1.1 Purpose

This manual is a guide for process engineers, information technology personnel, operations managers and other plant personnel responsible for developing and maintaining the cyber-security for DeltaV distributed control system.

This manual describes the security features built into DeltaV systems and explains how to harden DeltaV installations against cyber-security threats. This manual supports installation and maintenance of DeltaV software. It includes descriptions of patching, backup and restore activities, and procedures for verifying that security mechanisms for hardening the DeltaV system have been properly installed and configured.

1.2 Organization

The remainder of this introduction provides references to related documents and contains a glossary of security related terminology.

Section 2 describes basic security concepts and provides guidance for working with IT and Emerson Process Management personnel to apply these concepts. It also provides guidance on determining the need for having security policies and procedures for a given installation.

Section 3 describes the as-built security features of DeltaV systems.

Section 4 describes how to patch DeltaV systems.

Section 5 discusses backup and recovery activities of DeltaV systems.

Section 6 describes installation and maintenance from a security perspective.

Finally, the individual topics described in this manual may refer the reader to other DeltaV documentation that contains additional detail.

1.3 Relevant documentation

1.3.1 Background reading

The following whitepapers provide introductory material for understanding digital security:

- Best Practices for DeltaV Cyber Security
- DeltaV Cyber Security
- Emerson Wireless Security - WirelessHART® and Wi-Fi™ Security
- Report: M 2784 – X – 10, Process Control Domain – Security Requirements for Vendors, published by WIB, Second issue, October 2010, version 2.0

Although no system can be made completely free from security risks, risk can be reduced in the following ways:

- Develop a comprehensive security policy for the DeltaV system.
- Follow the guidelines in this manual.
- Provide training for employees.
- Make digital security an ongoing process through continuous reevaluation of security risks and rigorous implementation of security practices that make sense for the system.

1.3.2 DeltaV documentation

The documentation that describes the various aspects of the DeltaV system are listed below.

- *DeltaV Books Online*: the main, online reference for details on DeltaV implementation. It is available on the DeltaV product media and is a free-standing application that can be obtained separately for planning the system implementation.
- *Installing Your DeltaV Distributed Control System* and *Getting Started with Your DeltaV Digital Automation System* manuals: provide information on hardware setup and overviews of the DeltaV system architecture and applications. These manuals are available on paper and in DeltaV Books Online.
- Whitepapers: provide information on a variety of topics. They are typically free-standing documents covering a single topic. Whitepapers provide detailed information to help users better understand product functionality or implementation. They are available from Emerson.
- Product data sheets: specify product capabilities and functionality. They are available from Emerson.
- Knowledge-Based-Articles (KBA): provide up-to-date information on implementing a DeltaV distributed control system. They are available to Foundation Support customers on the secure support site.

1.3.3 Microsoft documentation

DeltaV systems incorporate many of the security features provided by the Microsoft Windows operating system and supporting software elements. For the details of how to configure and operate this software, consult the Microsoft documentation.

1.3.4 3rd party product documentation

DeltaV systems support three levels of integration of 3rd party products: tightly integrated (e.g. Cisco switches), approved for integration (e.g. Symantec Endpoint Protection), and Emerson Process Management Alliance products (e.g. OSI Pi).

For tightly integrated products, documentation is included in *DeltaV Books Online* and in KBAs as appropriate. This documentation includes very specific directions for implementing tightly integrated products to provide the most robust DeltaV system solution. Deviations from this documentation can result in non-supported solutions.